Protecting Your Privacy and Money in a Hi-Tech World

Howard County Office of Consumer Protection

Howard County Office of
Consumer Protection

October is National Cyber Security Awareness Month

Advances in technology have made it easier to shop, bank and connect with friends.

But it also makes it easier for hackers and other crooks to access your personal information and steal your money.

3 simple steps to help protect yourself

- Change the password for your most sensitive accounts frequently;
- Update your software and operating systems;
- Don’t give out personal information (e.g. financial account numbers, PINs, social security or health insurance info) unless you are sure who you are dealing with!

Email

- **Beware of phishing emails –**
  - **Appear to be from legitimate companies or financial institutions and ask for personal information;**
  - **Often contain links to fake websites - e.g. "We suspect an unauthorized transaction on your account. To ensure that your account has not been compromised, clink on the link and confirm your identity;"**
  - **May ask you to "confirm" by email your personal information.**

Email

- Don’t open email from anyone you do not know. “Spam” emails are sent as bait;
- If you mistakenly open an email from someone you don’t know, do not reply, click on links or call phone numbers provided in message. Links install malware that collects information that can be sold or used to commit identity theft;

Email continued

- **Do not participate in chain email. Participants usually placed on "sucker lists;"**
- **Don't email financial information – (e.g. credit card, checking account or social security number) especially if you are using an "open" network.**

Texting

- **Spam texts are like spam email - Promise free gifts so you will reveal personal information;**
- **Ignore texts from unknown senders. Don't click links. Delete messages that ask for personal information;**
- **Place your cell number on the National Do Not Call Registry, 888-382-1222, or go to www.donotcall.gov to reduce telemarketing calls.**

Social Media

- 64% of on-line adults 50-64 and nearly 50% 65 and older use Facebook (AARP). Social media phishing has more than doubled in the past year;
- Crooks look for personal information on social media they can use to pose as someone you know and trust - then ask for money or additional personal information that can be used to steal your identity - e.g. grandparent scams;
- Crooks may use the info themselves or sell it to others

Social Media- Never Share

- **Social security number; full birth date, mother's maiden name, home address or phone numbers;**
- **Current whereabouts or other info that can be used to trace you;**
- **Info that reveals when your home is unoccupied or children are home alone.**

Common Social Media Scams – Customer Service Imposters

- **Crook creates a social media account using a reputable company's name with the addition of an extra character (e.g. Targets) and monitors the real company's account for questions or complaints;**
- **The crook responds quickly with a link to its (fake) website that asks for log-in info and account number, or other personal information;**
- **Customers are so happy to get an immediate response they don't question whether the response is legit.**

Common Social Media Scams – Live-streaming fakes

- **Crooks offer free viewing of a big game, popular concert, etc.;**
- **Provide link – but before starting the stream, the site asks for credit card number for a "free trial" offer that can be cancelled at any time;**
- **Once you provide the info, you find out the stream doesn't work but you've already given your info.**

Common Social Media Scams - Discount offers

- **Crooks create fake social media page that looks like a legit company's and offers free or deeply discounted products;**

- **But you have to provide contact and other personal information, along with your credit card number (to pay for shipping and handling).**

Common Social Media Scams

- **Surveys and contests**
  - **Crook offers a prize for completing a survey;**
  - **Survey asks for personal info that the crook can use later to pose as a family member, friend or company you follow.**

- **Family member imposters.**

Surfing the Internet

- **Be mindful when signing up for newsletters or agreeing to terms; read the fine print to avoid receiving junk mail, telemarketing calls and spam;**
- **Don't click on pop ups and beware of spoofing – websites created by imposters to imitate sites of well-known companies;**
- **Don't take claims at face value – use Snopes or other sites to see if claims are true.**

Shopping Online

- **Shop on secure sites, look for a URL that begins with https. Choose strong passwords that are unique and not easily guessed by others;**

- **Do independent research to confirm the seller's physical address and phone number. Are there complaints or other indications that the company is scam?**

Shopping Online

- **Read descriptions thoroughly. Comparison shop-compare shipping and handling fees, refund policies, and delivery dates.**

- **Pay by credit card so you can dispute the charge if a problem arises.**

Chip Credit and Debit Cards

- **Nationwide shift by major card issuers to enhance security against fraud.**
- **US consumers make 24% of all credit card sales, but are responsible for 50% of fraud worldwide;**
- **Chip or EMV cards (short for Europe Mastercard and Visa) look like your old cards but also have a small square metallic chip on the front.**

Advantages of Chip Cards

- **Provides greater protection of your credit card number.**
  - **The chip does not hold your credit card number but instead the chip creates a unique code for each purchase.**
  - **Since your card number is not communicated to the merchant, there's less risk of the number being stolen;**

- **Can be used outside the US. Europe and other countries have been using since 2002.**

Disadvantages of Chip Cards

- Chips alone don't go far enough. If your card is lost or stolen, it can still be used in stores (easy to forge signatures) or on-line since all of the info needed is on the card;
- Other countries require PINs. A credit card thief won't know the PIN so can't complete the transaction on-line or in person;
- In the meantime, consider using "enhanced authentication" for on-line purchases.

Enhanced Authentication

- **2-step authentication – in addition to PINs and/or security questions, the bank sends a unique code by text or email that must be entered;**
- **A Biometric authenticator – that uses your camera for finger print to verify that it's you. These are typically found on new mobile devices, tablets or PCs;**
- **Use a security key - a small device that must be plugged into your USB port to log in to specified accounts.**

Mobile Banking

- Offered by banks, credit card companies to give consumers easy access to their accounts. Use to:
  - Deposit checks;
  - Pay bills;
  - Transfer funds;
  - Review account balances and recent transactions.

- Consumers can use their personal computers and/or smart phones apps.

Advantages of Mobile Banking

- You can access your account using your cellular phone service or through wi-fi;
- Using your smartphone or tablet for basic transactions makes it easy to keep an eye on finances without a trip to the bank;

Advantages of Mobile Banking

- **Mobile Banking is available 24/7, 365 days a year;**

- **Some banks will alert you when your balance goes below a certain dollar amount that you set.**

Disadvantages of Mobile Banking – Security Concerns

Ways to Avoid Unauthorized access:

- **Only access your account using a secured wireless network. Never use a free open network, like the ones at a coffee shop or restaurant;**
- **"Password protect" your phone so that if it gets lost or stolen, your mobile banking (and other apps) can't be accessed;**
- **Use enhanced authentication if possible.**

Using Shopping and Payment Apps

- **Apps - downloadable software that enhances the functionality of your smartphone or tablet - e.g. maps/directions, music, social media;**

- **Apps can access other info on your devise. Read the app's privacy and data use policy and adjust your settings to match your comfort level or find a different app;**

Helpful Shopping Apps

- **Price comparison apps can check best available price in real time. Scan product code and app searches online databases for price and other info about similar products sold online or in other stores;**
- **Coupon Apps help you find, earn or redeem coupons or loyalty points when shopping at specific stores;**
- **BUT, these apps collect info on shopping habits and may sell that info to others.**

In-Store Payment Apps

- **Enable you to pay for purchases from your phone or tablet using a bar code or QR (quick response) code;**
- **The app is linked to your credit, debit, gift or pre-paid card. Some apps charge your card for each purchase while others allow you to store value on the app.**

Before Downloading a Payment App

- Comparison shop by reading about the app's features, its terms and conditions and privacy and security policies;
- Pick security settings that provide the greatest protection;
- While payment apps usually use security safeguards such as firewalls and data encryption, consider enhanced authentication for using these apps.

Payment Apps - Billing Errors or Unauthorized Charges – Who Can Help?

- **The store can often help especially if it's an app developed by the retailer. Talk to customer service ASAP and ask for a supervisor if the employee can't help. Keep a record of who you talked to, when and what you are told.**

Payment Apps - Billing Errors or Unauthorized Charges – Who Can Help?

- The app company – most generally don't offer much help and some specifically say they will take no responsibility. So when considering an app, look at its help section, FAQs or terms of use for:
  - contact info;
  - how quickly you have to report problems;
  - any limits on your responsibility for unauthorized charges;
  - if the company will investigate problems and how long it will take.

Payment Apps - Billing Errors or Unauthorized Charges – Who Can Help?

- Your credit or debit card – if your card is charged for each purchase, your cards provide the same protection as with other purchases.

  Your responsibility for unauthorized charges is limited to:

  - $50 for credit card purchase;
  - For debit cards, responsibility is limited to $50 if reported within 2 business days after discovery; $500 if reported > 2 days but < 60 days after your statement that first shows the problem.

- But, if money is stored on the app you are responsible for the loss unless otherwise stated.

Peer to Peer Payment Apps – Allow you to pay friends or individuals on-line

- Comparison shop by reading about the app's features, its terms and conditions and privacy and security policies;
- Pick security settings that provide the greatest protection;
- Use enhanced authentication if possible;
- If tied to social media, make sure your payment history and other info is not accessible.

Helpful Resources

For more information on scams or any other consumer protections issue, contact:

Howard County Office of Consumer Protection

410-313-6420

consumer@howardcountymd.gov

www.howardcountymd.gov/consumer